UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/748,406	12/29/2003	Bo-Heung Chung	51876P554	7550

8791 7590 11/12/2008
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2435	
MAIL DATE	DELIVERY MODE
11/12/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/748,406	**Applicant(s)** CHUNG ET AL.	
	Examiner YOGESH PALIWAL	**Art Unit** 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 11 August 2008.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-10 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-10 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) □ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

- Applicant’s amendment filed on 08/11/2008 has been entered. Applicant has amended claims 1, 3, 6 and 8. Currently claims 1-10 are pending in this application.

Response to Arguments

1. Applicant's arguments filed 08/11/2008 have been fully considered but they are not persuasive.

- Applicant argues that “Amended Claims 1 and 6 more specifically point out the operations of setting and resetting of a first global variable and a second global variable during the change of a current intrusion detection rule. Marron and Huima do not teach or suggest these operations. Rather, Marron discloses the use of two transaction processing systems to coordinate dynamic changes to a computing system; one transaction processing system for processing old transactions and the other for processing new transactions (col. 3, lines 34-42). Marron does not disclose the operations of setting and resetting of a first global variable and a second global variable during the change of a current intrusion detection rule. Huima does not supply the missing elements. Huima is relied on for disclosing the use of a set of global variables to indicate a change to an intrusion detection rule. Huima discloses the use of a new rule during code execution (paragraph 31). However, Huima does not disclose setting a first global variable when the replica of the current intrusion detection rule is changed into a new intrusion detection rule, setting a second global variable and resetting the first global variable after the replica is changed, and resetting the second global variable when exchanging the current intrusion detection rule with the replica. Thus, Marron in view of Huima does not teach or suggest each of the elements of amended Claims 1 and 6, as well as their respective dependent claims, namely, Claims 2-4 and 5-9."

- In reply examiner would like to point out that Marron discloses setting a first global variable (see, Abstract, "The markers are set initially to unsafe.") when changing the replica of the old program into a new program in response to a request from a user area for updating the old program. (see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42, for detailed explanation, refer to "Response to Arguments" section) and resetting the first global variable after the replica is changed (see, abstract, "when all tasks are safe, the new programs replace the old programs") and Huima discloses Huima discloses a packet scanner system in which filter rules are changed dynamically and further discloses setting a second global variables after changing the replica to indicate to packet received after step b) that a change to the intrusion detection rule is in process and the packet is to use the new intrusion detection rule; and resetting the second global variable when exchanging the current intrusion detection rule with the replica and using the new intrusion detection rule on the packet (see Fig. 1, and paragraph 0031). The combination of Marron and Huima still discloses all the limitations of claims 1 and 6. Therefore, the rejection maintained.

Claim Rejections - 35 USC § 103

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-4, 6-9 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron (US 5359730) in view of Huima (US 20040015905 A1).

Regarding **Claims 1 and 6**, Marron discloses method and the inherent corresponding computer program for dynamically changing software module in a kernel level, the method comprising the steps of:

a) generating a replica of the old program in a kernel area **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42, for detailed explanation, refer to "Response to Arguments" section);**

b) setting a first global variable (see, Abstract, "The markers are set initially to unsafe.") when changing the replica of the old program into a new program in response to a request from a user area for updating the old program. **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42, for detailed explanation, refer to "Response to Arguments" section);** and b1) resetting the first global variable after the replica is changed (see, Abstract, “When all tasks are safe, the new programs replace the old programs”)

c) changing a currently applied program with the old program with using new program for the tasks **(Column 8, lines 49-52).**

Marron discloses a method of dynamically making software changes in a running system; however he does not teach dynamically changing an intrusion detection rule in a running system. Even though Marron discloses first global variables that mark all the tasks unsafe while the update is in progress and then mark them safe when new program replace the old program, Marron does not explicitly disclose setting a second global variables after changing the replica to indicate to packet received after step b) that a change to the intrusion detection rule is in process and the packet is to use the new intrusion detection rule; and resetting the second global variable when exchanging the current intrusion detection rule with the replica and using the new intrusion detection rule on the packet..

However, Huima discloses a packet scanner system in which filter rules are changed dynamically and further discloses setting a second global variables after changing the replica to indicate to packet received after step b) that a change to the intrusion detection rule is in process and the packet is to use the new intrusion detection rule; and resetting the second global variable when exchanging the current intrusion detection rule with the replica and using the new intrusion detection rule on the packet (see Fig. 1, and paragraph 0031).

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to apply the method of Marron to dynamically update kernel level intrusion detection rules of Huima *to non-disruptively install new versions of operating system [intrusion detection rules] modules while the system is running and one or more processes are executing which use and access such modules* (Marron, Column 5, lines 25-55). It would have been further obvious to include into the combined system a step of setting global variables to indicate to packet received after starting update that a change to the intrusion detection rule is in process and the packet is to use the new intrusion detection rule as further taught by Huima so that packet would be filtered according to the latest filtering rules thus improving the overall security.

Regarding **Claims 2 and 7**, the rejection of claims 1 and 6 is incorporated and further combination of Marron and Huima discloses a step of generating a replica of the new program [currently applied updated software] **(see Column 2, lines 67-68; Column 3, lines 1-6; Column 6, lines 50-53; and Column 3, lines 38-42,** Since Marron system require to do any update on a running code to be first performed on a copy of the code, it is implied that for performing any future update on the newly applied code, it would generate another copy and repeat the same process again to update currently new code to reflect any future updates**).**

Regarding **Claims 3 and 8**, the rejection of claims 1 and 6 is incorporated and the combination of Marron and Huima further discloses in the step b) and the step c), a change state of the intrusion detection rule [software] with a set of pre-assigned global variables is shown and the current intrusion detection rule [software] is changed according to the set of pre-assigned global variable **(Marron, Column 5, lines 35-41 as combined with Huima, Fig. 1, and paragraph 0031)**

Regarding **Claims 4 and 9**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Huima discloses that the kernel area transfers the request of changing the intrusion detection rule [updating the software] from the user area by using a system call **(Marron, Column 7, lines 25-28)**

Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Marron in view of Huima and further in view of Stoica (PHD thesis, “Stateless Core: A scalable Approach for Quality of Service in the Internet, Publication date: 12/15/2000)

Regarding **Claims 5 and 10**, the rejection of claims 3 and 8 is incorporated and further combination of Marron and Huima discloses that the kernel area transfers the intrusion detection result **(Huima, Paragraph 0011)** to an application program of a host, the intrusion detection rule being applied to the intrusion detection result **(Huima, Paragraph 0011).**

The combination of Marron and Huima does not disclose that the intrusion detection result being transferred by setting the global variables inside the kernel and determining the transferring position inside the kernel.

However, Stoica, in the same field of endeavor of kernel level monitoring system discloses that the kernel area transfers the kernel-monitoring log by setting the global variables inside the kernel and determining the transferring position inside the kernel

(Page 139, lines 19-21, "To minimize the monitoring overhead, we use the ip_output function call to send this information directly from kernel to an external monitoring machine.")

Therefore, it would have been obvious at the time the invention was made to one of ordinary skill in the art to send the intrusion detection results of the Marron and Huima combination from kernel to an external device by setting the global variables inside the kernel and determine the transferring position inside the kernel, as taught by Stoica, *to minimize the monitoring overhead and it also avoids unnecessary context switching between the kernel and the user level* **(Stoica, Page 139, lines 19-21)**

Conclusion

3. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435